We claim:

1. A method of implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the method comprising:

receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;

decrypting the received multicast traffic with the global key to produce decrypted multicast traffic;

encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain.

2. The method according to claim 1, further comprising:

receiving a global key message that identifies the global key.

3. The method according to claim 1 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

4. The method according to claim 1 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

5. The method according to claim 1 wherein the local key is only available to the given multicast domain.

6. The method according to claim 1 wherein the given multicast domain is a protocol independent multicast domain.

7. The method according to claim 1 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

8. The method according to claim 1 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

9. A method of implementing multicast security in a given multicast domain, the method comprising:

receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;

determining that the given multicast domain contains no network devices interested in the received multicast traffic; and

sending a terminate message to no longer forward the received multicast traffic to the given multicast domain.

10. The method according to claim 9, further comprising:

receiving a global key message that identifies the global key.

11. The method according to claim 9, further comprising:

determining, after having sent the terminate message, that the given multicast domain contains one or more network devices interested in the received multicast traffic; and

sending a resume message to once again forward the received multicast traffic to the given multicast domain.

12. The method according to claim 9 wherein the given multicast domain is a protocol independent multicast domain.

13. The method according to claim 9 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

14. The method according to claim 9 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

15. A method of implementing multicast security in a network, the method comprising:

encrypting multicast traffic with a global key, the global key being available to a given multicast domain and one or more other multicast domains;

forwarding the global encrypted multicast traffic to the given multicast domain;

receiving the global encrypted multicast traffic at the given multicast domain;

decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic;

encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

forwarding the local encrypted multicast traffic to one or more network devices in the given multicast domain.

16. The method according to claim 15, further comprising:

receiving at the given multicast domain a global key message that identifies the global key.

17. The method according to claim 15 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

18. The method according to claim 15 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

19. The method according to claim 15 wherein the local key is only available to the given multicast domain.

20. The method according to claim 15 wherein the given multicast domain is a protocol independent multicast domain.

21. The method according to claim 15 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

22. The method according to claim 15 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

23. A method of implementing multicast security in a given multicast domain, the method comprising:

receiving multicast traffic;

constructing, in response to the received multicast traffic, an information message that alerts other multicast domains of the security capabilities of the given multicast domain; and

forwarding the information message to at least one other multicast domain.

24. The method according to claim 23 wherein the information message is a part of a multicast protocol message.

25. The method according to claim 24 wherein one or more bits in one or more fields of the multicast protocol message are set to alert other multicast domains of the security capabilities of the given multicast domain.

26. An apparatus for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the apparatus comprising:

a receiver for receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;

a decryptor for decrypting the received multicast traffic with the global key to produce decrypted multicast traffic;

an encryptor for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

a traffic forwarder for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain.

27. The apparatus according to claim 26, further comprising:

a second receiver for receiving a global key message that identifies the global key.

28. The apparatus according to claim 26 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

29. The apparatus according to claim 26 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

30. The apparatus according to claim 26 wherein the local key is only available to the network devices in the given multicast domain.

31. The apparatus according to claim 26 wherein the given multicast domain is a protocol independent multicast domain.

32. The apparatus according to claim 26 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

33. The method according to claim 26 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

34. A computer program product for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the computer

program product comprising a computer usable medium having computer readable program code thereon, the computer program code including:

program code for receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;

program code for decrypting the received multicast traffic with the global key to produce decrypted multicast traffic;

program code for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

program code for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain.

35. The computer program product according to claim 34, further comprising:

program code for receiving a message that identifies the global key.

36. The computer program code to claim 34 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

37. The computer program code according to claim 34 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

38. The computer program code according to claim 34 wherein the local key is only available to the network devices in the given multicast domain.

39. The computer program code according to claim 34 wherein the given multicast domain is a protocol independent multicast domain.

40. The computer program code according to claim 34 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

41. The method according to claim 34 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

42. An apparatus for implementing multicast security in a network, the apparatus comprising: means for encrypting multicast traffic with a global key, the global key being available to a given multicast domain and one or more other multicast domains;

means for forwarding the global encrypted multicast traffic to the given multicast domain;

means for receiving the global encrypted multicast traffic at the given multicast domain;

means for decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic;

means for encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

means for forwarding the local encrypted multicast traffic to one or more network devices in the given multicast domain.

43. The apparatus according to claim 42, further comprising:

means for receiving at the given multicast domain a global key message that identifies the global key.

44. The apparatus according to claim 42 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

45. The apparatus according to claim 42 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

46. The apparatus according to claim 42 wherein the local key is only available to the given multicast domain.

47. The apparatus according to claim 42 wherein the given multicast domain is a protocol independent multicast domain.

48. The apparatus according to claim 42 wherein the given multicast domain is a group of contiguous protocol independent multicast domains.

49. The method according to claim 42 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.